DOI: https://doi.org/10.30525/2256-0742/2025-11-2-142-149

ELECTRONIC (DIGITAL) EVIDENCE COLLECTION IN ECONOMIC CRIME INVESTIGATIONS

Artem Kovalenko[1], Volodymyr Kovalenko[2], Yehor Nazymko[3]

Abstract. The increasing computerisation of the economic sector has led to a growing reliance on electronic document workflow, digital information exchange, and online financial transactions by both enterprises and individuals. These developments have also led to the computerisation and digitalisation of economic crime. It is an inevitable consequence of such offences that distinctive electronic (digital) traces are left behind. These traces may be recognised as electronic (digital) evidence and necessitate specialised procedures by law enforcement bodies. Therefore, the *purpose of this article* is to identify and present the main criminal procedural and forensic means of electronic (digital) evidence collection in economic crime investigations. The study's *methodology* is founded upon a range of general and special methods of scientific cognition. Utilising the formal-legal method, the authors analysed the content of current criminal procedural legislation and established the essence of electronic (digital) evidence. The formal-logical method enabled the authors to differentiate between procedural and forensic means of collecting electronic (digital) evidence. The modelling method assisted in constructing hypothetical models of investigators' behaviour while collecting electronic (digital) evidence in economic crime investigations, among other applications. The *results* of the study demonstrate that current Ukrainian criminal procedure legislation does not define electronic (digital) evidence; rather, it establishes electronic documents as procedural sources of proof and provides for the legal framework of examining computer data. In accordance with the prevailing provisions of the Ukrainian Criminal Procedure Code, the primary modus operandi for the procurement of electronic (digital) evidence entails the meticulous examination of computer data. This process entails the authorised individual's meticulous observation of the data content, culminating in the systematic documentation of the findings within an official protocol. In the course of economic crime investigations, a wide range of electronic documents are typically subject to inspection. These documents contain information pertaining to the business activities of the subjects under investigation. It is recommended that the execution of this procedural action be entrusted to professionals specialising in both computer technology and software, in addition to those versed in economic principles. The utilisation of forensic expert examination constitutes a pivotal instrument in the process of acquiring electronic (digital) evidence during the course of economic crime investigations. The possession of computer-technical expertise can facilitate access to protected files, the recovery of deleted or damaged data, and the retrieval of specific information from vast data sets. The meticulous examination of telecommunications systems and devices is a pivotal method of extracting information from the network equipment used by offenders. The application of forensic economic expertise facilitates the analysis of previously seized electronic records, enabling the evaluation of their significance in the investigation of economic crime.

Keywords: economic crimes, pretrial investigation, proving, electronic (digital) evidence, investigative (search) actions, forensic tactics, computer data inspection, forensic examination.

JEL Classification: K14, K24, K42

[1] Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine *(corresponding author)*
E-mail: new4or@gmail.com
ORCID: https://orcid.org/0000-0003-3665-0147
[2] Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine
E-mail: kvvkrimluvd@ukr.net
ORCID: https://orcid.org/0000-0001-5310-2092
[3] Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine
E-mail: nazumuch@ukr.net
ORCID: https://orcid.org/0000-0003-4949-4155

1. Introduction

It is evident that economic activity, both within Ukraine and worldwide, is undergoing comprehensive computerisation and digital transformation. In particular, following the implementation of qualified electronic (digital) signatures, enterprises of all ownership forms are gradually abandoning the physical (paper) format of official documentation. In the contemporary era, the processing of all work-related information in electronic format is a far more convenient process. It is evident that almost all sectors of production have undergone computerisation and automation, and consequently, data regarding production processes is now almost exclusively stored in digital format. Information exchange frequently occurs online via the Internet, as opposed to face-to-face interactions. The circulation of funds is increasingly conducted in electronic form, and the governments of some countries are significantly restricting the use of cash for business transactions. This policy is often termed the "war on cash", and its introduction is intended to combat crime and provide central banks with greater scope for monetary policy manoeuvre (Dowd, 2019).

Concurrently, illegal economic activities, which are subject to criminal liability, are also becoming computerised. According to scholars in the field, economic crimes are defined as a broad spectrum of offences outlined in criminal law, pertaining to the implementation of illegal economic activity (economic processes, relations, operations) and the violation of government or international regulations governing legal economic activity (Kyrgizova, 2024). This category encompasses a wide range of illicit activities, including various forms of smuggling, customs fraud, tax crimes, obstruction of lawful economic activity, financial fraud, securities forgery, insider trading, money laundering, and numerous other offences. It is also important to note that a broader interpretation of the category of economic crimes exists, which, in addition to those mentioned above, encompasses crimes against property, including offences such as fraud, extortion, embezzlement, and the misappropriation or unlawful acquisition of property, and so forth (Cherniavskyi et al., 2021, p. 422).

The digitalisation of the entire economic sector has compelled criminals to store and use their own information in electronic form, while also finding advantages in this for their illicit activities. In particular, offenders have long been concealing "black accounting" on remote servers and cloud file-hosting services (De Busser, 2019, p. 1257), in order to protect themselves from the exposure of sensitive data in the event of searches at their locations. Furthermore, cryptocurrencies, electronic funds and e-payment systems are the most common tools used to legalise criminal income (Nazymko, Volobuieva & Kryzhanovskyi, 2023, p. 202).

The aforementioned trend has enabled researchers to distinguish financial cybercrime as a discrete category, encapsulating the convergence of financial crime, hacking and social engineering in cyberspace for the exclusive purpose of illegal economic gain (Nicholls, Kuppa & Le-Khac, 2021). However, even traditional economic crimes may also be enabled by, or dependent on, internet-connected systems and digital technologies, and thus inherently possess a clear "cyber" aspect. Nevertheless, this does not render them "pure" cybercrimes (Lord & Levi, 2023, p. 3). Consequently, at this current stage, it is inevitable that every economic crime will leave distinct electronic (digital) traces, which must be detected, documented, and thoroughly examined by authorised individuals. The information contained in such traces is considered to be evidentiary in legal proceedings in the form of electronic (digital) evidence, which requires specific approaches to their collection.

In consideration of the aforementioned, the **objective of the present article** is to establish and present the primary criminal procedural and forensic means of electronic (digital) evidence collection in economic crime investigations.

2. The Essence of Electronic (Digital) Evidence under Current Ukrainian Criminal Procedural Legislation

The current Criminal Procedure Code of Ukraine (hereinafter referred to as the CPC of Ukraine) is distinctive in that, in contrast to commercial, civil, and administrative legislation, it does not provide a separate definition of electronic (digital) evidence. However, it should be noted that this does not imply a disregard by law enforcement officers for potentially evidentiary information that exists in computer-based form during investigations.

In the contemporary context of criminal proceedings, investigators routinely engage with computer data that has been generated or modified in relation to the crime under investigation. These data contain information about the status and performance of a specific computer system (a single device or network) and therefore make it possible to trace the actions performed by a particular user on these computers. Such data constitute specific electronic (digital) traces, which scholars define as materially invisible traces that can be detected, recorded, and studied by digital electronic devices and contain any forensically relevant material information recorded in electronic digital form on physical media (Golovin et al., 2022, p. 161). In the majority of cases, the evidence obtained includes office documents created or edited by individuals who have been implicated in the crime

in question. Other forms of evidence may include emails, instant messages, digital photographs and video recordings (including footage from surveillance cameras and in-car video recorders), web pages, operating system files, and a wide variety of other data.

In order for certain information to acquire evidentiary status and be admissible in court, authorised persons must identify, examine and record it in strict accordance with the requirements of the law. Computer data acquires the status of a procedural source of evidence – an electronic document – after examination in accordance with Article 237(1) and (2) of the CPC of Ukraine (The Criminal Procedure Code of Ukraine, 2012). The Code states that documents may exist and be used in electronic form in Article 99, but it does not provide an interpretation for this type of document. The legal definition of this term is provided in Article 5 of the Law of Ukraine "On Electronic Documents and Electronic Document Management," according to which an electronic document is defined as a document in which information is recorded in the form of electronic data, including the mandatory requisites of the document (The Law of Ukraine "On Electronic Documents and Electronic Document Management", 2003).

Under the current legislation, computer data may be considered electronic documents, provided that their content meets the requirements of Article 99(1) of the CPC of Ukraine (i.e., they are deliberately created for the purpose of storing information, contain data recorded by means of written signs, sound, images, etc. that may be used as evidence of facts or circumstances established in criminal proceedings). It is evident that computer data, by definition, signifies specific information that has been deliberately encoded in a format comprehensible to a computer. Consequently, they predominantly fall under the broader category of electronic documents.

In accordance with Articles 84 and 99 of the Ukrainian Criminal Procedure Code, documents are classified as a distinct category of criminal procedural evidence. In accordance with global standards, electronic forms of documentation are generally accepted as valid evidence, encompassing text messages, emails, and computer-generated reports (Ingram, 2021, p. 19). However, this methodology is a recent development within the Ukrainian criminal justice system. It is an established fact that computer data is typically encoded in digital form and processed through the movement of electrons in computer equipment. Consequently, evidence based on such data is commonly referred to as either electronic or digital. It is this author's opinion that these terms should be combined in order to demonstrate both key technologies that, at the current stage, underlie computer data.

It is evident that computer data cannot exist in isolation; rather, they are intrinsically linked to their physical carriers. Hard disk drives (HDDs) and solid-state drives (SSDs), in addition to optical discs and memory flash cards, are all examples of data storage media. Notwithstanding the fact that the investigator may access information available on the Internet using a work computer, it is imperative that they bear in mind that the original data is stored on the hard drive of a server located elsewhere. Conversely, a pivotal attribute that differentiates electronic documents as electronic (digital) evidence from conventional physical evidence (objects and paper documents) is their capacity to be fully and immutably duplicated and disassociated from the physical medium. Consequently, Ukrainian legislation acknowledges electronic documents as valid substitutes for originals, contingent upon the fulfilment of all technical and legal requirements during the copying process.

It follows that, in principle, the collection of electronic (digital) evidence can be undertaken in two distinct ways: either by seizing the physical medium containing the data (or the entire computer device), or by making a copy of the data. The primary option is undoubtedly preferable, as it ensures the integrity of the original medium by protecting it from unauthorised alterations or destruction. There may, however, be cases where law enforcement agencies do not have physical or legal access to the storage medium (for example, when the server is located abroad), or where the court does not authorise the seizure of the storage medium. In particular, Article 168 of the CPC of Ukraine establishes the general rule that law enforcement officers must copy the data and leave the original storage media in the possession of the owners, except in certain complex situations. In such a scenario, the copies of the computer data must be used for evidentiary purposes.

It is evident that electronic (digital) evidence in Ukrainian criminal proceedings comprises information in the form of computer data. This data has been obtained by authorised persons in accordance with the procedures established by current legislation. Therefore, the presence or absence of facts and circumstances relevant to the criminal proceedings and subject to proof is determined by the investigator, prosecutor, investigating judge and court.

The procedural form of such evidence (its procedural source) is the aforementioned electronic document (Art. 99(3) and (4) of the CPC of Ukraine). The evidentiary information is derived from computer data, which are electronic (digital) traces of a criminal offence, while the medium of information is the physical carrier of computer data (Kovalenko, 2024, p. 108).

3. Tactical and Organisational Means of Collecting Electronic (Digital) Evidence in Economic Crime Investigations

The main tactical tool for collecting electronic (digital) evidence under current Ukrainian law is the inspection of computer data. This investigative (detective) action is regulated by Article 237(1) and (2) of the CPC of Ukraine and consists in the authorised person's perception of the content of such data and recording the information received in the relevant protocol.

Consequently, data stored on the original medium (CD, DVD, USB, SSD, HDD, flash memory, etc.) or located on remote servers, including those accessible via the Internet, can be detected and analysed. In the event of computer data hosted on a network being subjected to examination, its inspection constitutes a discrete procedural action. In cases involving the examination of data stored on a physical medium or in the memory of specific computer hardware, the inspection process may be integrated with a procedural action, provided that lawful access to the objects in question has been obtained. Therefore, the examination of computer data may take place as part of a crime scene inspection, a search, the obtaining of temporary access to items and documents, certain covert investigative actions (searches), and other procedural activities.

It is important to acknowledge the high degree of sensitivity that financial information of individuals and enterprises possesses. Consequently, data protection legislation is applicable to safeguard this data from unlawful or incorrect processing (De Busser, 2019, p. 1252). In accordance with Ukrainian legislation, access to such information is contingent upon judicial authorisation.

During economic crime investigations, typical objects of computer data inspection include the following:

– Corporate electronic documents (contracts, invoices, accounting records, reporting forms, orders and other administrative acts, official letters, etc.). These documents typically follow a specific format and structure and are often certified with a qualified electronic signature, which allows for verification of their authenticity.

– Draft and unofficial electronic documents are defined as any data stored by individuals or enterprise personnel in text, spreadsheet, or other types of files. In contradistinction to official documentation, these do not adhere to standardised internal structures, mandatory fields, or formatting conventions. Authorship and authenticity can be determined through a combined analysis of the primary content and file metadata.

– Information about financial transactions on the bank accounts of individuals or companies. Such data can of course be obtained from banks in paper form, either at the request of law enforcement authorities or by court order. However, given the overall digitisation of the financial sector and the large volumes of information involved, such data is now predominantly stored and processed in electronic form.

– Cryptocurrency wallets and accounts in electronic payment systems.

– Corporate and personal email correspondence of individuals or company employees.

– Official websites of companies and their verified social media profiles. Such data can provide information about the declared and actual directions of their economic activity.

– Footage from surveillance cameras installed at company premises or in public places.

– Personal social media profiles of individuals involved in the investigation. The content of these profiles may provide evidence of the individual's presence in particular locations, associations with other persons, or possession of undeclared assets.

In the course of an inspection of computer data in criminal proceedings related to economic offences, it is necessary to involve specialists from two main categories. The initial category encompasses specialists in the domain of computer hardware and software products. Such an individual possesses the requisite education and the necessary skills to proficiently operate computer hardware and the software installed on it. The primary function of the specialist during the inspection of computer data is to ensure the integrity of the original data, assist with searching for specific information, and copy the data to specially prepared media. Article 99(4) of the CPC of Ukraine requires the involvement of such a specialist when copying computer data so that these copies are equated to the originals and acquire evidentiary value as electronic documents. The specialist might also use various techniques and forensic applications to search hidden folders, retrieve deleted data, decrypt the data, restore damaged files, etc. (Ombu, 2023, p. 60). However, such complex operations should rather be entrusted to forensic experts. Concurrently, there is concurrence with researchers that the investigator should possess the requisite knowledge in the domain of information technology to facilitate effective engagement and collaboration with relevant specialists during the pre-trial investigation (Cherniavskyi et al., 2021, p. 430).

The second category should include a specialist in economics, as it would be difficult for an investigator or prosecutor to identify the specific information relevant to the investigation of an economic crime within the vast array of data in electronic (digital) form. It is evident that this necessitates specialised economic knowledge, which is not typically anticipated among procedural actors. An engaged economic specialist may provide consultations regarding the types of data

that may contain significant financial information, explain their content, identify connections between documents, and assist in preparing materials for the subsequent appointment of a forensic economic expertise.

By their inherent character, computer data embody encoded information, inherently imperceptible to human senses, necessitating interpretation through the utilisation of computer technology. Accordingly, during the inspection of computer data, authorised personnel and involved specialists must employ appropriate technical tools, including but not limited to: computer hardware (e.g., personal computers, laptops, tablets); network equipment (e.g., routers, switches); data output devices (e.g., monitors, speakers, headphones, virtual reality headsets); and specialised software capable of interpreting specific types of data.

The fundamental equipment necessary for the purpose of inspecting computer devices and computer data comprises the following: a portable computer with an autonomous power source; reserve battery kits; a CD-ROM (DVD-ROM) drive; disks containing operating systems and other software tools; data storage devices, including a medium with a capacity that exceeds that of the device being examined; a hard drive blocker and/or a duplicator set; screwdrivers and other tools; a portable forensic field kit, and so forth (Vinakov et al., 2017).

A significant element of the inspection of computer data is the documentation of the information obtained during the process. The documentation of such procedures is conducted through a verbal description of the course and the results of the procedural action in the relevant protocol. Additionally, the examined data or its specific parts are copied and preserved.

The introductory section of the protocol should include the location, date and time of the inspection, identification of all participants, information about the involved specialists (including their qualifications), and a description of the scientific and technical tools used – such as computer hardware, specialised equipment, and software. The descriptive section of the protocol meticulously documents each action undertaken by the authorised individual with the computer equipment, along with the information procured as a consequence. Each examined file must be described in detail, including its format, size, directory location on the original storage medium, other relevant metadata, and the actual content of the data it contains. The final part of the computer data inspection protocol, in accordance with the general requirements of the Criminal Procedure Code of Ukraine, must include a description of the methods used to preserve the obtained data. This section should include a detailed account of the procedure by which the data were copied.

It is imperative that the computer data under scrutiny is copied and transferred to a storage medium that has been prepared in advance. The storage medium selected depends on the volume of data; CD/DVD discs, flash drives, HDDs, and other storage devices may be used. In order to verify the integrity and authenticity of the copied data, it is recommended that both the original data and its copies be hashed, followed by a comparison of the resulting hash values (Kalancha & Harkusha, 2021, p. 338).

Another procedural instrument for obtaining electronic (digital) evidence is the covert investigative (search) action of "extracting information from electronic information systems" (Article 264 of the CPC of Ukraine). This is a process that is undertaken in instances where law enforcement authorities require the concealment of the fact of accessing suspects' computer equipment. Furthermore, it is employed in situations that necessitate the covert circumvention of logical or physical protection measures applied to computer data. In all other cases, it is advisable to conduct an overt inspection of computer data. A specific tool for financial investigations is the covert investigative (search) action of "monitoring of bank accounts" (Article 269(1) of the CPC of Ukraine). At the same time, it should be noted that the use of covert procedural measures to form electronic (digital) evidence in economic investigations requires separate doctrinal research.

4. Forensic Expertise as Means to Collect and Examine Electronic (Digital) Evidence in Economic Crime Investigations

The seizure of data carriers and computer equipment from enterprises can be regarded as physical evidence in economic crime cases. However, the primary evidential value of such items lies in the information stored within their memory.

Nonetheless, there may be circumstances in which investigators have already gained physical access to the data carrier, yet, for various reasons, are unable to independently (or with the assistance of a specialist) inspect the computer data stored in its memory. Such an occurrence may be observed in instances where technical means to examine the contents of the carrier are not available (e.g., where the required connection interface or software is unavailable), when bypassing logical protection (e.g., passwords, encryption) is necessary, when data recovery is required, when partially damaged equipment needs to be restored, or when data volumes are too large. In such cases, the medium may be sent for examination within the scope of a *forensic expertise of computer hardware and software* (also referred to as *computer-technical expertise*). It is advisable to send original carriers of computer data, their full (bitwise) copies, or computer devices seized in a criminal proceeding for such an examination.

Typical tasks performed by experts include: 1) determining the technical condition (functionality) of computer hardware; 2) searching for and identifying information stored on electronic media; 3) recovering deleted information; 4) tracing the user's network activity, visited Internet resources, search queries and message exchange history; 5) analysing the user's actions and software operations within the computer system; 6) analysing the mobile phone's memory, which involves examining: the user's message history in communication applications (messengers, social networks), application usage history, file download and upload history, call history and SMS text messages (Stepaniuk & Kolesnyk, 2023, p. 294).

For instance, the mobile devices of individuals under investigation are often protected by multiple layers of security, ranging from standard passwords to biometric locking and data encryption. In most cases, circumventing such protection requires the utilisation of specialised software and hardware tools, which are not typically accessible to investigators or specialists. Concurrently, mobile phones serve as a repository for critical information, including call records, SIM contacts, incoming messages, multimedia messaging service and short message service, images, video, audio, chats, documents, and network information (Borysenko et al., 2021, p. 141). Consequently, in instances where an investigator suspects that significant information pertinent to a financial investigation may be present in the memory of such a device, it is recommended to seek the expertise of forensic experts.

Another typical issue in financial investigations is the attempt by suspects to destroy computer data that could be used as evidence against them. The level of computer proficiency exhibited by the offender dictates the methods employed in the data deletion process. These methods include the utilisation of operating system tools, the infliction of damage to computer equipment or data carriers, and the deployment of specialized software for the purpose of deep data erasure. In the most elementary of cases, such information may be recovered by a specialist during the inspection of computer data. In other situations, the investigator should appoint a forensic examination.

In the context of economic crime investigations, a pivotal aspect of computer-technical forensic examination pertains to the identification of specific information on computer data carriers. These data carriers characteristically encompass substantial volumes of data. In the event that a forensic expert is furnished with particular keywords and search criteria, said expert will be capable of extracting the information relevant to the prosecution from the general data set. Prior to delegating the task of locating pertinent data to a forensic expert, it is incumbent upon the investigator to seek consultation from a specialist in economics. It is imperative that the specialist is provided with the available case materials and copies of documents seized from the suspects for the purpose of review, in order to facilitate the formulation of appropriate keywords. The latter may include specific numerical values (monetary amounts), electronic and physical addresses, the nomenclature of enterprises, the nomenclature of officials, product categories, and other relevant identifiers. Pursuant to the findings of the computer-technical examination, the expert will be in a position to furnish the investigator with information regarding specific files that contain the requested data. These files can then be examined by the investigator in co-operation with an economic specialist.

If the prosecution is interested in information regarding the operation of network equipment used by the subjects of the investigation, it is appropriate to appoint an *expertise of telecommunication systems and devices*. The key tasks of such an examination include determining the characteristics and technical condition of telecommunication systems and devices; identifying the means used for processing, transmitting, and securing data within these systems; establishing the occurrence and methods of access to telecommunications systems, resources, and data; and reconstructing the content of information that was transmitted, received, or processed by such devices.

Furthermore, no economic crime investigation can proceed without conducting a *forensic economic expertise*. Firstly, the engagement of an expert to determine the amount of damages in criminal proceedings on economic crimes is obligatory (Hloviuk, Hryniuk & Kovalchuk, 2019, p. 384). Secondly, the specialised knowledge of a forensic expert is instrumental in providing investigators with answers regarding the nature and specifics of the suspects' economic activities, which is crucial for proving their guilt. The examination is comprised of three distinct components: the forensic expertise of accounting documents, the forensic expertise of taxation documents, and the forensic expertise of financial and credit transaction documents. In this context, the direct objects of forensic economic expertise may include previously collected electronic (digital) evidence. Such evidence may take the form of documents containing information about the financial activities of individuals or businesses who may be involved in the commission of a crime.

5. Conclusions

Thus, one of the trends in the development of the economic sphere is its complete digitalisation and computerisation. Both companies and individuals are increasingly abandoning the physical (paper) form of official documents, resorting to storing work-related information in electronic formats, communicating online via the Internet, conducting financial transactions

electronically, and so on. Consequently, the digitalisation of economic crime is becoming increasingly prevalent. Offenders are storing and manipulating information electronically, concealing their data on cloud storage platforms, coordinating their activities via online platforms, and laundering illicit financial proceeds through cryptocurrencies and e-payment systems. It is evident that all economic crimes leave behind distinctive electronic (digital) traces, which must be detected, collected, and examined by law enforcement authorities and used as electronic (digital) evidence in economic investigations.

The prevailing Ukrainian criminal procedural legislation does not delineate a discrete concept of electronic (digital) evidence. Nevertheless, electronic documents are admissible as evidence, provided that they have been obtained by authorised individuals in strict compliance with the law and contain information relevant to the criminal proceedings. It can be posited that these documents are constituted of computer data in essence. In the event of their creation or alteration in connection with a criminal offence, they are regarded as electronic (digital) traces of the crime.

The primary procedural and tactical instrument for the collection of electronic (digital) evidence is the inspection of computer data. This investigative (search) action involves the direct perception of the content of such data by an authorised person and the documentation of the obtained information in the appropriate protocol. In the course of economic crime investigations, objects of inspection commonly include official and unofficial documents of enterprises in electronic format, information about the financial transactions on the bank accounts, corporate and personal electronic correspondence of individuals, web pages and social media profiles, surveillance camera footage, and so on. It is recommended that the involvement of specialists in the fields of computer technology and software products, as well as economics, be considered during the execution of such a procedural action. The documentation of the process and results of computer data inspection is achieved through the provision of a verbal description of the procedure in the protocol, and the subsequent copying and preservation of the examined data or its individual components.

In criminal proceedings pertaining to economic crimes, electronic (digital) evidence is also collected during forensic expert examinations. The field of computer-technical expertise is concerned with the retrieval of valuable information from encrypted, protected, deleted, or damaged computer data, as well as with other complex cases. Law enforcement agencies are able to obtain information about the operation of the offenders' network equipment through the expertise of telecommunication systems and devices. Forensic economic expertise constitutes the primary tool for the analysis of the content of previously collected electronic evidence in terms of its relevance to the investigation of economic offences.

In view of the aforementioned points, it is hypothesised that further research into the methodology of conducting computer data inspections and other investigative (search) actions during economic crime investigations is a promising avenue for future research.

References:

Borysenko, I. V., Bululukov, O. Yu., Pcholkin, V. D., Baranchuk, V. V., Prykhodko, V. O. The Modern Development of New Promising Fields in Forensic Examinations. *Journal of Forensic Science and Medicine*, 7(4), 137–144. DOI: https://doi.org/10.4103/jfsm.jfsm_66_21

Cherniavskyi, S., Babanina, V., Vartyletska, I., & Mykytchyk, O. (2021). Peculiarities of The Economic Crimes Committed with the Use of Information *Technologies. European Journal of Sustainable Development*, 10(1), 420–431. DOI: https://doi.org/10.14207/ejsd.2021.v10n1p420

De Busser, E. (2019). EU-US Digital Data Exchange to Combat Financial Crime: Fast is the New Slow. *German Law Journal*, 19(5), 1251–1267. DOI: https://doi.org/10.1017/S2071832200023026

Dowd, K. (2019). The war on cash is about much more than cash. *Economic Affairs*, 39(3), 391–399. DOI: https://doi.org/10.1111/ecaf.12377

Golovin, D., Nazymko, Ye., Koropatov, O., Korniienko, M. (2022). Electronic Evidence in Proving Crimes of Drugs and Psychotropic Substances Turnover. *Access to Justice in Eastern Europe*, 2 (14), 156–166. DOI: https://doi.org/10.33327/AJEE-18-5.2-n000217

Hloviuk, I., Hryniuk, V. & Kovalchuk, S (2019). Modern Challenges to Engagement an Expert in Criminal Proceedings on Economic Crimes in Ukraine. *Amazonia Investiga*, 8 (23), 378–385. Available at: https://amazoniainvestiga.info/index.php/amazonia/article/view/881

Ingram, Jefferson L. (2021). Criminal Evidence. 14th edition. Routledge, New York.

Kalancha, I. H. & Harkusha, A. M. (2021). Copy of Electronic Information as Evidence in Criminal Proceedings: Procedural and Technical Aspects. *Legal Scientific Electronic Journal,* 8, 336–339. DOI: https://doi.org/10.32782/2524-0374/2021-8/77

Kovalenko, A. V. (2024). Forensic Doctrine on the Collection, Examination, and Use of Evidence in Criminal Proceedings. Kyiv: Alerta.

The Law of Ukraine "On Electronic Documents and Electronic Document Management" No. 851-IV. *Verkhovna Rada of Ukraine*, 2003. Available at: https://zakon.rada.gov.ua/laws/show/851-15

The Criminal Procedure Code of Ukraine. The Law of Ukraine of 13.04.2012 No. 4651-VI. *Verkhovna Rada of Ukraine*, 2012. Available at: https://zakon.rada.gov.ua/laws/show/4651-17

Lord, N. & Levi, M. (2023). Economic crime, economic criminology, and serious crimes for economic gain: On the conceptual and disciplinary (dis)order of the object of study. *Journal of Economic Criminology*, 1, 100014. DOI: https://doi.org/10.1016/j.jeconc.2023.100014

Kyrgizova, V. S. (2024). The concept of economic crimes in legal doctrine and legislation, and their differentiation. *Analytical and Comparative Jurisprudence*, 5, 710–715. DOI: https://doi.org/10.24144/2788-6018.2024.05.109

Nazymko, E., Volobuieva, O., & Kryzhanovskyi, O. (2023). Prevention of legalisation (laundering) of criminal proceeds in the mechanism of ensuring economic security of the state. *Baltic Journal of Economic Studies*, 9(4), 198–205. DOI: https://doi.org/10.30525/2256-0742/2023-9-4-198-205

Nicholls, J., Kuppa, A., & Le-Khac, N. -A. (2021). Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. *IEEE Access*, 9, 163965–163986. DOI: https://doi.org/10.1109/ACCESS.2021.3134076

Ombu, A. (2023). Role of Digital Forensics in Combating Financial Crimes in the Computer Era. *Journal of Forensic Accounting Profession*, 1(3), 57–75. DOI: https://doi.org/10.2478/jfap-2023-0003

Stepaniuk, R., & Kolesnyk, V. (2023). Forensic computer and technical expertise: state and prospects of development. *Bulletin of Luhansk State University of Internal Affairs named after E. Didorenko*, 2(102), 289–305. DOI: https://doi.org/10.33766/2524-0323.102.289-305

Vinakov, A., Huzii, V., Davis, D., Dubyna V., et al. (2017). Detection, Prevention, and Investigation of Human Trafficking Crimes Committed through the Use of Information Technologies: A Training Course. Kyiv.

Received on: 20th of March, 2025
Accepted on: 26th of April, 2025
Published on: 20th of May, 2025